Claims

The claims are listed as follows:

1. (Original) A key management device for provision of a security service in an Ethernet-based passive optical network, comprising:

an optical line terminal for sending a discovery gate message to discover an optical network unit for data transmission, and, if said optical network unit receives said discovery gate message and then requests data communication, sending an encrypted registration message including a permanent medium access control (MAC) address of said optical network unit to said optical network unit to notify said optical network unit that it has been registered and an encrypted general gate message including said permanent MAC address of said optical network unit to said optical network unit to allocate a time slot to said optical network unit; and

said optical network unit for receiving said discovery gate message and then sending an encrypted registration request message to said optical line terminal to request the data communication therewith and an encrypted registration acknowledgement message to said optical line terminal to respond to said registration message.

2. (Original) The key management device as set forth in claim 1, wherein said discovery gate message is periodically sent.

3. (Original) The key management device as set forth in claim 1, wherein said discovery gate message includes a time slot field allocated to said optical network unit for registration thereof, a capability of said optical line terminal, a public key of said optical line terminal, and a nonce encrypted by a private key of said optical line terminal for signature.

4. (Original) The key management device as set forth in claim 1, wherein said registration request message includes a physical ID capability, a capability of said optical network unit, an echo of a capability of said optical line terminal, a session key, a nonce decrypted by a public key of said optical line terminal, and a nonce created for signature of said optical network unit.

5. (Original) The key management device as set forth in claim 4, wherein said physical ID capability, said capability of said optical network unit, said echo of said capability of said optical

line terminal, said nonce decrypted by said public key of said optical line terminal and said nonce created for the signature of said optical network unit are encrypted using said session key.

6. (Original) The key management device as set forth in claim 4, wherein said session key is encrypted using said public key of said optical line terminal.

7. (Original) The key management device as set forth in claim 1, wherein said registration message further includes a physical ID list, an echo of a capability of said optical network unit, and a signature of said optical network unit.

8. (Original) The key management device as set forth in claim 1, wherein said general gate message further includes a time slot field for upstream transmission of said optical network unit.

9. (Original) The key management device as set forth in claim 8, wherein said general gate message is encrypted using a session key.

10. (Original) The key management device as set forth in claim 1, wherein said registration acknowledgement message includes a session key encrypted by a public key of said optical line terminal, and an echo of a registered physical ID.

11. (Original) The key management device as set forth in claim 10, wherein said registration acknowledgement message is encrypted using said session key.

12. (Original) The key management device as set forth in claim 1, wherein said optical line terminal includes:

a public key processor for creating a public key to be included in said discovery gate message, and encrypting and decrypting said public key;

a session key processor for decrypting said registration request message and registration acknowledgement message from said optical network unit using a session key, and encrypting said general gate message and registration message using said session key;

a private key processor for creating a private key using said public key for encryption of messages to be transmitted to said optical network unit and decryption of messages received from said optical network unit, and encrypting and decrypting said private key; and

storage means for storing and managing said public key, session key and private key.

13. (Original) The key management device as set forth in claim 1, wherein said optical network unit includes:

a session key processor for creating a session key for encrypted communication with said optical line terminal, encrypting a part of said registration request message using said session key, decrypting said registration message and general gate message from said optical line terminal using said session key and encrypting said registration acknowledgement message using said session key;

a public key processor for encrypting said session key using a public key from said optical line terminal; and

storage means for storing said session key and public key.

14. (Original) A method for session key distribution between an optical line terminal and an optical network unit in a key management method for provision of a security service in an Ethernet-based passive optical network, comprising the steps of:

a), by said optical line terminal, sending a discovery gate message to discover said optical network unit for data transmission;

b), by said optical network unit, receiving said discovery gate message and then sending an encrypted registration request message to said optical line terminal to perform data communication therewith;

c), by said optical line terminal, sending an encrypted registration message including a permanent MAC address of said optical network unit to said optical network unit to notify said optical network unit that it has been registered;

d), by said optical line terminal, sending an encrypted general gate message including said permanent MAC address of said optical network unit to said optical network unit to allocate a time slot to said optical network unit; and

e), by said optical network unit, sending an encrypted registration acknowledgement

message to said optical line terminal to respond to said registration message.

15. (Original) The session key distribution method as set forth in claim 14, wherein said discovery gate message is periodically sent.

16. (Original) The session key distribution method as set forth in claim 14, wherein said discovery gate message includes a time slot field allocated to said optical network unit for registration thereof, a capability of said optical line terminal, a public key of said optical line terminal, and a nonce encrypted by a private key of said optical line terminal for signature.

17. (Original) The session key distribution method as set forth in claim 14, wherein said registration request message includes a physical ID capability, a capability of said optical network unit, an echo of a capability of said optical line terminal, a session key, a nonce decrypted by a public key of said optical line terminal, and a nonce created for signature of said optical network unit.

18. (Original) The session key distribution method as set forth in claim 17, wherein said physical ID capability, said capability of said optical network unit, said echo of said capability of said optical line terminal, said nonce decrypted by said public key of said optical line terminal and said nonce created for the signature of said optical network unit are encrypted using said session key.

19. (Original) The session key distribution method as set forth in claim 17, wherein said session key is encrypted using said public key of said optical line terminal.

20. (Original) The session key distribution method as set forth in claim 14, wherein said registration message further includes a physical ID list, an echo of a capability of said optical network unit, and a signature of said optical network unit.

21. (Original) The session key distribution method as set forth in claim 14, wherein said general gate message further includes a time slot field for upstream transmission of said optical

network unit.

22. (Original) The session key distribution method as set forth in claim 21, wherein said general gate message is encrypted using a session key.

23. (Original) The session key distribution method as set forth in claim 14, wherein said registration acknowledgement message includes a session key encrypted by a public key of said optical line terminal, and an echo of a registered physical ID.

24. (Original) The session key distribution method as set forth in claim 23, wherein said registration acknowledgement message is encrypted using said session key.

25 – 28. (Canceled)

29. (Withdrawn) A method for key recovery between an optical line terminal and an optical network unit in a key management method for provision of a security service in an Ethernet-based passive optical network, comprising the steps of:

a) determining whether a pair of private and public keys are in error;

b), if said pair of private and public keys are in error, by said optical line terminal, creating a pair of new private and public keys and multicasting the new public key while including it in a desired message; and

c), by said optical network unit, receiving said new public key, comparing it with a public key pre-stored in a public key storage unit therein, discarding said new public key if it is the same as the pre-stored public key and storing said new public key in said public key storage unit if it is different from the pre-stored public key.

30. (Withdrawn) The key recovery method as set forth in claim 29, wherein said step a) includes the step of, by said optical line terminal or optical network unit, detecting a private/public key error by decrypting a received message using a session key and verifying a frame check sequence for the decrypted message.

31. (Withdrawn) The key recovery method as set forth in claim 29, wherein said new public key created by said optical line terminal is sent to said optical network unit while being included in a discovery gate message.

32. (Withdrawn) A method for key recovery between an optical line terminal and an optical network unit in a key management method for provision of a security service in an Ethernet-based passive optical network, comprising the steps of:

a) determining whether there is a session key error between said optical line terminal and said optical network unit; and

b), if there is a session key error between said optical line terminal and said optical network unit, by said optical network unit, sending a new session key to said optical line terminal using a time slot sent while being included in a discovery gate message.

33. (Withdrawn) The key recovery method as set forth in claim 32, wherein said step a) includes the step of determining that there is a session key error between said optical line terminal and said optical network unit, if there is not continuously present any upstream transmission from said optical network unit pre-allocated a time slot from said optical line terminal.

34. (Withdrawn) The key recovery method as set forth in claim 32, wherein said step a) includes the step of determining that there is a session key error between said optical line terminal and said optical network unit, if said optical network unit periodically receives said discovery gate message from said optical line terminal, but does not continuously receive a general gate message from said optical line terminal.

35. (Withdrawn) The key recovery method as set forth in claim 32, wherein said new session key created by said optical network unit is sent to said optical line terminal while being included in a report message.